

Inhaltsverzeichnis

Empfehlungen zur englischen Originalausgabe	13
Geleitwort zur englischen Originalausgabe unter dem Titel Decrypting Money	15
Geleitwort zur deutschen Ausgabe	19
Weshalb es dieses Buch gibt	21
Teil 1: Die Geschichte des Geldes	29
1 Die Ursprünge des Geldes	31
1.1 Warengeld	31
1.1.1 Kaurimuscheln	32
1.1.2 Rai-Steine	32
1.1.3 Römische Denare	34
1.1.4 Zigarettenwährung	36
1.2 Repräsentatives Geld	36
1.2.1 Papiergeld	37
1.2.2 Das britische Pfund	38
1.2.3 Drei neue Probleme	38
1.3 Fiat-Geld	41
1.4 Geld und der Staat	42
1.4.1 Zentralbanken	42
1.4.2 Privates Geld	43
1.4.3 Freies Bankensystem	44
1.5 Zusammenfassung des Kapitels	45
2 Die Funktionen und Eigenschaften von Geld	47
2.1 Drei Funktionen des Geldes	47
2.1.1 Ein Tauschmittel	47
2.1.2 Eine Rechnungseinheit	48
2.1.3 Ein Wertaufbewahrungsmittel	48
2.2 Eigenschaften von Geld	49
2.2.1 Knappheit	49
2.2.2 Haltbarkeit	50
2.2.3 Tragbarkeit	50
2.2.4 Teilbarkeit	50
2.2.5 Fungibilität	51
2.2.6 Sicherheit und Fälschungen	51

2.3	Bewertung von Geld nach Funktionen und Merkmalen	53
2.3.1	Kaurimuscheln	53
2.3.2	Rai-Steine	53
2.3.3	Römische Denare	53
2.3.4	Zigaretten-geld	54
2.3.5	Repräsentatives- und Fiat-Geld	54
2.3.6	Vergleich der verschiedenen Währungen	55
2.4	Zahlungssysteme	55
2.5	Zusammenfassung des Kapitels	57
3	Die Digitalisierung des Geldes	59
3.1	Digitale Zahlungssysteme	60
3.2	Digitale Fiat-Währungen	62
3.3	Digitale Privatwährungen	63
3.3.1	E-Gold	63
3.3.2	Liberty Dollar	64
3.3.3	Linden Dollar	65
3.3.4	DigiCash	65
3.3.5	B-Money	65
3.3.6	Bitgold	66
3.3.7	Hashcash	66
3.4	Kryptowährungen und Bitcoin	67
3.5	Zusammenfassung des Kapitels	67
	Teil 2: Bitcoin, die erste Kryptowährung	69
4	Bitcoin-Geschichte	71
4.1	Satoshi Nakamoto	71
4.1.1	Seine Identität	71
4.1.2	Sein Genie	72
4.1.3	Seine Agenda	73
4.2	Der Beginn von Bitcoin	81
4.2.1	Das Whitepaper	82
4.2.2	Frühzeitige Bewertungen	83
4.3	Zusammenfassung des Kapitels	84
5	Bitcoin-Struktur	85
5.1	Die Bitcoin-Währung	85
5.1.1	Knappheit	85
5.1.2	Teilbarkeit	87
5.1.3	Haltbarkeit	87
5.1.4	Übertragbarkeit	88

5.1.5	Fungibilität	88
5.1.6	Vergleich von Merkmalen	88
5.2	Das Bitcoin-Zahlungssystem	89
5.2.1	Dezentralisiert und Peer-to-Peer	89
5.2.2	Möglichkeiten des Handels	90
5.2.3	Sicherheit	91
5.2.4	Offenes Protokoll und Open Source	91
5.2.5	Öffentliches Ledger	92
5.3	Eigenschaften von Bitcoin	92
5.3.1	Betriebszeit	92
5.3.2	Transaktionsentgelte	93
5.3.3	Stabilität	94
5.3.4	Pseudonymität	95
5.4	Probleme mit Bitcoin	97
5.4.1	Möglichkeit von Fehlern	97
5.4.2	Technische Risiken	98
5.4.3	Missbrauch	100
5.4.4	Illegaler Inhalt	100
5.4.5	Fehlender Rechtsbehelf	101
5.4.6	Mindestreserve-Bankwesen	101
5.4.7	Reputationsfragen	102
5.4.8	Möglichkeit staatlicher Eingriffe	103
5.5	Zusammenfassung des Kapitels	103
Teil 3: Wie Bitcoin funktioniert		105
6	Bitcoin-Grundlagen	107
6.1	Terminologie	107
6.1.1	Bitcoin-Adressen und privater Schlüssel	107
6.1.2	Das Bitcoin-Ledger	109
6.1.3	Bitcoin-Transaktionen	111
6.2	Bitcoin-Verwaltung	113
6.2.1	Bitcoin-Wallet	113
6.2.2	Die Wechseladresse	115
6.2.3	Konten und UTXOs	116
6.2.4	Unsaubere Bitcoins	118
6.2.5	Hierarchische deterministische Geldbörse	119
6.3	Art von Geldbörsen	119
6.3.1	Papier- und Metallgeldbörsen	120
6.3.2	Hardware-Geldbörsen	120
6.3.3	Software-Geldbörsen auf dem Computer (online/offline)	121

6.3.4	Mobiltelefon-Geldbörse	121
6.3.5	Online-Geldbörse	121
6.3.6	Brain Wallet	122
6.3.7	Zusammenfassung	122
6.4	Erwerb von Bitcoin	123
6.4.1	Kryptowährungsbörsen	124
6.4.2	Andere Mittel zum Erwerb von Bitcoin	125
6.5	Mining und Erzielung eines Konsenses	127
6.5.1	Transaktionsverarbeitung in einem zentralisierten System	127
6.5.2	Das Erreichen eines Konsenses in einem dezentralen System ist schwierig	129
6.5.3	Blöcke und Bitcoin-Mining	132
6.5.4	Das Bitcoin-Knoten-Netzwerk	135
6.6	Second Layer	136
6.7	Zusammenfassung des Kapitels	140
7	Kryptografische Primitive	141
7.1	Kryptografische Hashfunktionen	141
7.1.1	Eigenschaften	142
7.1.2	Anwendungen	145
7.2	Public-Key-Kryptografie	148
7.2.1	Sichere Kommunikation	148
7.2.2	Nachweis des Besitzes	150
7.3	Digitale Signaturen	151
7.3.1	Einzelne Signaturen	151
7.3.2	Public-Key-Kryptografie und Bitcoin	154
7.3.3	Signieren von Bitcoin-Transaktionen	155
7.3.4	Mehrere Unterschriften	156
7.4	Zusammenfassung des Kapitels	156
8	Bitcoin-Mining	157
8.1	Erstellung eines Blockkandidaten	157
8.1.1	Transaktionsauswahl	158
8.1.2	Der Blockkandidat	159
8.1.3	Coinbase-Transaktion	162
8.1.4	Der Block-Header	163
8.2	Aufbau eines Blockes	166
8.2.1	Zu viele Blöcke	166
8.2.2	Das mathematische Problem von Bitcoin	168
8.2.3	Hashrate	170
8.2.4	Proof of Work	171
8.2.5	Ziel-Hash und Schwierigkeitsanpassungen	172

8.3	Blockchain und Konsens	175
8.3.1	Die Blockchain	175
8.3.2	Die Längste-Kette-Regel	177
8.3.3	Bestätigungen	180
8.3.4	Der 51-Prozent-Angriff	181
8.3.5	Zusammenfassung	186
8.4	Die Wirtschaftlichkeit von Mining	186
8.4.1	Einkommen aus dem Mining	186
8.4.2	Die Netzwerk-Hashrate	191
8.4.3	Mining-Kosten	196
8.4.4	Geografie	198
8.5	Mining-Pools	199
8.6	Zusammenfassung des Kapitels	200
9	Bitcoin-Verbreitung	201
9.1	Anfänge	201
9.1.1	Frühe Bitcoin-Börsen	201
9.1.2	Volatilität	202
9.1.3	Frühzeitige Teilnehmer	203
9.1.4	Mainstream-Aufmerksamkeit	204
9.1.5	Multi-Signatur-Adressen	206
9.1.6	Blockgrößenkrieg	207
9.1.7	Ordinals und Inscriptions	211
9.1.8	Ökosystem der Kryptowährungen	213
9.2	Bitcoin und die traditionelle Finanzindustrie	214
9.2.1	Finanzinstitute	214
9.2.2	Bitcoin-Futures	215
9.2.3	Bitcoin-Fonds	216
9.2.4	Bitcoin-ETFs und ETNs	217
9.2.5	Einführung von Bitcoin Spot ETFs in den USA	217
9.2.6	Verwendung in Unternehmens- und Staatskassen	218
9.3	Zusammenfassung des Kapitels	219
Fazit	221
Glossar	225
Literaturverzeichnis	231
Weitere Literaturempfehlungen	233
Bildnachweise	235
Stichwortverzeichnis	237
Danksagungen	241
Über die Autoren	243